Universidade de Brasília Faculdade UnB Gama

Criptografia e Segurança de Redes
Trabalho 1

Alunos: Matrículas:
João Paulo Nunes Soares 15/0038267
Josué Nascimento da Silva 15/0038933

- INSTRUÇÕES DE USO
  - **Exercício 1**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc main.c -o main** .
    - Para executar o programa execute: **./main**
    - **OBS:**
      - Para que o programa execute de forma correta dois arquivos são necessários: um arquivo contendo a mensagem e outro contendo a chave utilizada, onde a chave deve ter o tamanho máximo de 64 bits e a mensagem tendo seu valor em multiplos de 64 (ex: 64,128,…)
      - O arquivo de entrada da mensagem deverá ser nomeado como : ***entradaMensagem.txt*** e o arquivo contendo a chave a ser utilizada deverá ser nomeado como ***entradaChave.txt*** .
      - Em ambos devem ser utilizados caracteres hexadecimais.
      - A função de encriptação irá gerar o arquivo com a mensagem cifrada, onde o mesmo será utilizado pelo programa na decifração.
      - Antes de selecionar a função de decifração, deverá ser realizado a função de encriptação.
      - Garanta que o arquivo *generatekeys.c* estará na mesma pasta do arquivo *main.c* ao compilar.
  - **Exercício 2**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc main.c -o main** .
    - Para executar o programa execute: **./main**
    - Após executar, insira os valores na ordem solicitada e a resposta será mostrada.
  - **Exercício 3**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc main.c -o main** .
    - Para executar o programa execute: **./main**
    - Após executar o programa, insira os dois valores em que se deseja realizar uma operação, e depois escolha uma das opções disponíveis.A resposta será mostrada no terminal.

- LIMITAÇÕES CONHECIDAS
  - **Exercício 1**
    - A mensagem de entrada deve ter o número de bits da mensagem igual a n*64, onde n é maior ou igual a 1.Ou seja, o número de bits deverá ser igual a uma das opções: 64,128,192,…
    - Quando utilizado caracteres alfabéticos eles deverão estar em formato minusculo.Exemplo: a,b,c,d,e …

- ✔ **Exercício 2**
  - ✔ Não existem limitações conhecidas
- ✔ **Exercício 3**
  - ✔ A função de divisão não está totalmente implementada.

- ◆ DIVISÃO DO TRABALHO
  - ✔ Ambos os alunos realizaram a atividade, onde a maior parte foi realizada no modelo de pareamento.